IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.:	10/686,956	**Art Unit:**	2121
Inventors:	Singer *et al.*	**Examiner:**	DUNN, Darrin D.
Filed:	October 15, 2003	**Confirmation No.:**	8803
Title:	**CONTENT ACCESS IN A NETWORK MEDIA ENVIRONMENT**	**Docket No.:**	113748-4837US

APPEAL BRIEF (37 C.F.R. § 41.37)

Mail Stop Appeal Brief - Patents
US Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is an Appeal from the rejection of claims 1-3 and 5-39 in the final office action of August 5, 2010, relating to the above-referenced application.

(i) Real Parties in Interest

Sony Corporation and Sony Pictures Entertainment Inc., assignees of the present application, are the real parties in interest.

(ii) Related Appeals and Interferences

There are no related appeals and/or interferences currently pending.

(iii) Status of Claims

Claims 1-3 and 5-39 are pending in the case. Claims 1-3 and 5-39 have been rejected. Claims 1-3 and 5-39 are appealed herein.

The present application was filed on October 15, 2003 with claims 1-40. In an amendment dated February 1, 2008 (in response to the restriction requirement dated November 1, 2007), claim 40 was cancelled, and claims 1, 14, 19, 26, and 37 were amended. In an amendment dated September 2, 2008 (in response to the office action dated May 1, 2008), claims 1, 2, 4, 5, 7, 8, 14, 18, 19, 25, 26, 36, 37, and 39 were amended. In an amendment dated March 26, 2009 (in response to the office action dated November 28, 2008), claims 1, 2, 5-7, 14, 19, 21, 26, 32, and 37 were amended. In an amendment dated November 20, 2009 (in response to the office action dated July 22, 2009), claims 1, 14, 19, 26, and 37 were amended. In an amendment dated May 5, 2010 (in response to the office action dated February 5, 2010), claims 1, 14, 19, 26 and 37 were amended. In an amendment dated December 6, 2010 (in response to the office action dated August 5, 2010), no claims were amended. No further claim amendments have been made.

(iv) Status of Amendments

No further amendments were submitted after submitting a response (to the final office action dated August 5, 2010) dated December 6, 2010.

(v) **Summary of Claimed Subject Matter**

A. Claim 1 – A method of presenting content data, comprising:

a) receiving at a server device a present request indicating locked content data from a client connected to a hub network, (Specification as filed, page 4, lines 15-31; page 8, lines 20-29)

b) wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network, (Specification as filed, page 4, lines 15-31; page 5, lines 7-15)

c) wherein the server device is configured to function as a client in the hub network, and (Specification as filed, page 4, lines 15-31)

d) wherein said locked content data is stored on the server device connected to the hub network; (Specification as filed, page 5, line 20 to page 6, line 6)

e) checking a license corresponding to said locked content data to determine if said license permits said client to present said locked content data, (Specification as filed, page 5, line 20 to page 6, line 6)

f) wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said client connected to the hub network, (Specification as filed, page 5, line 20 to page 6, line 6)

g) wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and (Specification as filed, page 5, line 20 to page 6, line 6)

h) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network, (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

i) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled; and (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

j) presenting said locked content data through a presentation component connected to said client when said locked content data is a bound instance. (Specification as filed, page 5, lines 1-6)

B. Claim 2 – The method of claim 1, wherein

a) said locked content data and said license corresponding to said locked content data are stored on the server device. (Specification as filed, page 5, line 20 to page 6, line 6)

C. Claim 5 – The method of claim 1, wherein

a) checking said license includes sending a confirm license request to the server device from said client. (Specification as filed, page 5, line 20 to page 6, line 6)

D. Claim 7 – The method of claim 1, wherein

a) checking a revocation list to determine whether said client is included in said revocation list; (Specification as filed, page 19, line 25 to page 20, line 7)

b) wherein said revocation list indicates devices for which the license has been revoked, and (Specification as filed, page 19, line 25 to page 20, line 7)

c) wherein said revocation list is stored on said server device. (Specification as filed, page 19, line 25 to page 20, line 7)

E. Claim 14 – A method of presenting content data, comprising:

a) receiving at a server connected to a hub network a present request indicating locked content data and indicating to a client connected to said hub network to present the content data, (Specification as filed, page 4, lines 15-31; page 8, lines 20-29)

b) wherein the server is configured to set up the hub network including adding the client and the server to the hub network, (Specification as filed, page 4, lines 15-31; page 5, lines 7-15)

c) wherein the server is configured to function as a client in the hub network, and (Specification as filed, page 4, lines 15-31)

d) wherein said locked content data is stored on the server connected to the hub network; (Specification as filed, page 5, line 20 to page 6, line 6)

e) checking a license corresponding to said locked content data to determine if said license permits said server to present said locked content data through said client, (Specification as filed, page 5, line 20 to page 6, line 6)

f) wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said server through said client connected to the hub network, (Specification as filed, page 5, line 20 to page 6, line 6)

g) wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and (Specification as filed, page 5, line 20 to page 6, line 6)

h) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub

network, (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

i) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled; and (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

j) presenting said locked content data by streaming data to said client when said locked content data is a bound instance. (Specification as filed, page 5, lines 1-6)

F. Claim 19 – A method of copying content data, comprising:

a) receiving in a hub network a copy request indicating locked content data, (Specification as filed, page 5, line 20 to page 6, line 21)

b) wherein the hub network includes a server configured to set up the hub network including adding the client and the server to the hub network, and (Specification as filed, page 4, lines 15-31; page 5, lines 7-15)

c) wherein the server is configured to function as a client in the hub network and wherein said locked content data is stored on the server; and (Specification as filed, page 4, lines 15-31)

d) copying said locked content data to produce a copy of said locked content data when said locked content data is a bound instance with a corresponding license that is bound to said hub network; (Specification as filed, page 5, line 20 to page 6, line 6)

e) wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and (Specification as filed, page 5, line 20 to page 6, line 6)

f) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network, (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

g) the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled. (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

G. Claim 26 – A method of distributing content data, comprising:

a) receiving from a providing device connected to a hub network, and at a receiving device a copy of locked content data that is a bound instance bound to said hub network, (Specification as filed, page 6, lines 7-21; page 7, lines 19-25)

b) wherein the providing device is configured to set up the hub network including adding the receiving device and the providing device to the hub network, (Specification as filed, page 4, lines 15-31; page 5, lines 7-15)

c) wherein the providing device is configured to function as a receiving device in the hub network, and (Specification as filed, page 4, lines 15-31)

d) wherein said locked content data is stored on the providing device connected to the hub network; (Specification as filed, page 5, line 20 to page 6, line 6)

e) requesting a new license for said copy of locked content data; and (Specification as filed, page 5, line 20 to page 6, line 6)

f) receiving said new license for said copy of locked content data of the bound instance bound to said hub network, (Specification as filed, page 5, line 20 to page 6, line 6)

g) wherein the bound instance of said copy of locked content data and the new license corresponding to said copy of locked content data are bound to the hub network, and (Specification as filed, page 5, line 20 to page 6, line 6)

h) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network, the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled. (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

11. Claim 37 – A method of distributing content data, comprising:

a) receiving at a server connected to a hub network, and from a device a request for a new license for a copy of locked content data that is a bound instance bound to said hub network, (Specification as filed, page 4, lines 15-31; page 8, lines 20-29)

b) wherein the server is configured to set up the hub network including adding the client and the server to the hub network, (Specification as filed, page 4, lines 15-31; page 5, lines 7-15)

c) wherein the server is configured to function as a client in the hub network, and (Specification as filed, page 4, lines 15-31)

d) wherein said locked content data is stored on the server connected to the hub network; (Specification as filed, page 5, line 20 to page 6, line 6)

e) checking a root license stored on said server to determine if said root license permits said server to provide a new license for said copy of locked content data of the bound instance; and (Specification as filed, page 5, line 20 to page 6, line 6)

f) creating said new license according to said root license; (Specification as filed, page 5, line 20 to page 6, line 6)

g) sending said new license to said device, (Specification as filed, page 5, line 20 to page 6, line 6)

h) wherein said new license for said copy of locked content data of the bound instance is bound to said hub network, (Specification as filed, page 5, line 20 to page 6, line 6)

i) wherein the bound instance of said copy of locked content data and the new license are bound to the hub network, and (Specification as filed, page 5, line 20 to page 6, line 6)

j) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network, the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled. (Specification as filed, page 5, line 20 to page 6, line 6; p36, line 26 to page 37, line 18)

(vi) Grounds of Rejection to be Reviewed on Appeal

A. Whether claims 1-3 and 5-18 are unpatentable over Messerges et al. (U.S. Publication No. 20020157002; hereinafter referred to as "Messerges") in view over Foster et al. (U.S. Publication No. 20030198351; hereinafter referred to as "Foster"), in view over Chase et al. (U.S. Publication No. 20030187801; hereinafter referred to as "Chase"), and in further view over Yaacovi (U.S. Publication No. 20030018582; hereinafter referred to as "Yaacovi") under 35 U.S.C. §103(a).

B. Whether claims 19-28 are unpatentable over Messerges in view over Russell et al. (U.S. Publication No. 20020069420; hereinafter referred to as "Russell"), in view over Foster, in view over Chase, and in further view over Yaacovi under 35 U.S.C. §103(a).

C. Whether claims 29-39 are unpatentable over Messerges in view over Foster, and in further view over Russell, in view over Chase, in view over Yaacovi and in further view over Peinado et al. (U.S. Publication No. 20030217011; hereinafter referred to as "Peinado") under 35 U.S.C. §103(a).

(vii) Argument

A. Claims 1-3 and 5-18 are not unpatentable over Messerges in view over Foster, in view over Chase, and in further view over Yaacovi under 35 U.S.C. §103(a)

In the final office action dated August 5, 2010 ("the Office Action"), claims 1-3 and 5-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Messerges in view over Foster, in view over Chase, and in further view over Yaacovi. As explained in the Manual of Patent Examination Procedure §706.02, entitled Rejection on Prior Art, for obviousness under 35 U.S.C. §103, "to support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of

reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." As set forth in detail below, the outstanding rejections are improper because the cited references do not suggest the claimed invention either explicitly or impliedly, or the examiner did not present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the cited references.

Claim 1 recites a method of presenting content data, comprising:

(a) receiving at a server device a present request indicating locked content data from a client connected to a hub network,

(b) wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network,

(c) wherein the server device is configured to function as a client in the hub network, and

(d) wherein said locked content data is stored on the server device connected to the hub network;

(e) checking a license corresponding to said locked content data to determine if said license permits said client to present said locked content data,

(f) wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said client connected to the hub network,

(g) wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and

(h) wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network,

(i) the server device sends a disable request for the

locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled; and

(j) presenting said locked content data through a presentation component connected to said client when said locked content data is a bound instance.

(limitation designators added)

The limitations of claim 1 are disclosed in the specification in relation to the difference between the discrete and bound instances. For example, "[a]s discussed below, an instance that is compliant with hub network operation is in one of two exclusive states: discrete or bound. A discrete instance is independent of any hub network and can be played or presented through any compliant device (according to the license of the discrete instance). However, a compliant device cannot make a usable copy of a discrete instance. A discrete instance includes locked content data and a discrete license. The locked content data of the discrete instance is referred to as the "discrete version" of the locked content data. The locked content data is locked by being protected from unauthorized access, such as by encryption. A bound instance is bound to one hub network. The bound instance is one logical instance represented by locked content data and corresponding licenses stored on the server of the hub network and on zero or more of the clients of the hub network. The locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy versions" (though some or all of the data in the discrete version, the source version, and/or any of the sub-copy versions can be the same). A bound instance can only be played or presented through a compatible compliant device that is a member of that hub network. Members of that hub network can make sub-copies of the content data of a bound instance." *Specification of the application as filed, page 5, line 20 to page 6, line 6, emphasis added.*

Regarding limitations (a)-(d) of claim 1, they recite "receiving at a server device a present request indicating locked content data from a client connected to a hub network, wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network, wherein the server device is configured to function as a client in the hub network, and wherein said locked content data is stored on the server device connected to the hub network". These limitations are disclosed in the specification that "[t]he PVR 105 is a media network compliant device, meaning that the PVR 105 operates according to the processes defined for a device that is a member of a hub network. The PVR 105 includes storage for storing copies of content (e.g., as electronic files stored on a hard disk) and is a server device. As a server device, the PVR 105 is the server for a hub network and can provide content to client devices that are members in the hub network. As a server, the PVR 105 also defines a local environment (not shown). In this example, the local environment for the PVR 105 is defined as a physical area relative to the position of the PVR 105 (e.g., determined by round trip packet timing or GPS information). The PVR 105 is also a client device. As a client device, the PVR 105 can render content directly or through a connected terminal device, such as through the connected television 110. As both a client and server device, the PVR 105 is a member of a hub network as the server for the hub network and as a client in the hub network. In Figure 1, the PVR 105 is marked with "HN1" to indicate that the PVR 105 is a client device for hub network 1 (HN1)." *(Specification of the application as filed, page 4, lines 17-30).*

The specification also describes that "as a server device, the PVR 105 initially sets up the hub network HN1. The PVR 105 checks for other compliant devices connected to the PVR 105. Before adding a device as a member to the hub network HN1, the PVR 105 authenticates a device, confirming the identity of the device, and authorizes an authenticated device, confirming that the device is a compliant device. If the PVR 105 does not authenticate and authorize a device, the PVR 105 does not add that device to the hub network HN1. In Figure 1, the PVR 105 is the only compliant device. The PVR 105 adds itself to the hub network as the server and as a client. The television 110 is not a compliant device, and so the PVR 105 does not add the television 110 as a member.")."

(Specification of the application as filed, page 5, lines 7-15). The specification further describes that "the locked content data is locked by being protected from unauthorized access, such as by encryption. A bound instance is bound to one hub network. The bound instance is one logical instance represented by locked content data and corresponding licenses stored on the server of the hub network and on zero or more of the clients of the hub network. The locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy versions" (though some or all of the data in the discrete version, the source version, and/or any of the sub-copy versions can be the same)." *(Specification of the application as filed, page 5, line 26 to page 6, line 3).*

Regarding limitations (b)-(d), which recite "wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network, wherein the server device is configured to function as a client in the hub network, and wherein said locked content data is stored on the server device connected to the hub network," the Examiner states that these limitations are disclosed in paragraphs [0078] and [0080] of Foster. These paragraphs of Foster are recited below for reference (emphasis added):

> [0078] Although content can be freely shared among devices 202 A-E each device in the network 200 must still transmit the content in an encrypted format. Thus, each device receiving the content must perform the decryption on its own. Specifically, each device must determine the media key from the KMB, then use the media key in conjunction with the binding identifier and the authorization table to recover the binding key. The binding key will the decrypt the title key (or a title key-content usage condition combination), which will be used to decrypt and implement the underlying content.
>
> [0080] In general, a consumer can freely add compliant devices to his/her network 200 up to a predetermined amount. The process of adding a device to a consumer home network is as follows. A user connects a new xCP-

> enabled device to the network. The new device automatically generates a "who's there" message to determine which other xCP-enabled devices are in the network. Some of the existing devices on the network are authorizers and can authorize the new device. Also, some of the existing devices are servers meaning that they contain a copy of the network KMB and can share it with other devices. ...

Although the above paragraphs of Foster discloses that a consumer can freely add compliant devices to his/her network and that content must be transmitted in an encrypted format, they fail to teach or suggest limitations (b)-(d) of claim 1, namely that the server device sets up the hub network including adding the client, functions as a client in the hub network, and the locked content data is stored on the server device connected to the hub network.

Regarding limitations (h) and (i), they recite "wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network" and "the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled." These limitations are disclosed in at least following passages of the application as filed:

> [Page 5, line 20 to page 6, line 6] As discussed below, an instance that is compliant with hub network operation is in one of two exclusive states: discrete or bound. A discrete instance is independent of any hub network and can be played or presented through any compliant device (according to the license of the discrete instance). However, a compliant device cannot make a usable copy of a discrete instance. A discrete instance includes locked content data and a discrete license. The locked content data of the discrete instance is referred to as the "discrete version" of the locked content data. The locked content data is locked by being protected from unauthorized access, such as by encryption. A bound instance is bound to one hub network. The bound instance is one logical instance represented by locked content data and corresponding licenses stored on

> the server of the hub network and on zero or more of the clients of the hub network. The locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy versions" (though some or all of the data in the discrete version, the source version, and/or any of the sub-copy versions can be the same). A bound instance can only be played or presented through a compatible compliant device that is a member of that hub network. Members of that hub network can make sub-copies of the content data of a bound instance.
>
> [Page 36, line 26 to page 37, line 13] After the server receives the discrete request, the server causes the clients of the hub network to disable sub-copy versions of the corresponding bound instance, block 2515. The server sends a disable request to each of the members of the hub network, specifying for which bound instance sub-copy versions are to be disabled. Alternatively, the server sends the disable request to members that have sub-copy versions of the bound instance (e.g., as indicated through licenses sent to the clients). The clients receiving the disable request disable all sub-copy versions corresponding to the bound instance. By disabling a sub-copy version, compliant devices will not present or play the disabled sub-copy version. In one implementation, a client disables a sub-copy version by disabling the license for the sub-copy version. ...
>
> [Page 37, lines 14-18] After the server disables the sub-copy versions, the server disables the source version, block 2515. By disabling the source version, compliant devices will not present or play the source version. The server disables the source version similarly to the server disabling a discrete instance or a client disabling a sub-copy version, such as by disabling the root license for the bound instance.

Thus, limitations (h) and (i) state that when the locked content data is to be moved to another server device bound to another hub network, the locked content data is changed from a bound instance to a discrete instance. Further, the server device sends a disable request for the locked content data to the clients of the hub network to indicate that the

bound instance of the locked content data is changed to the discrete instance, and the disable request causes the license corresponding to the locked content data to be disabled.

The Office Action cites Chase, paragraphs [0020], [0279], [0283] and Yaacovi, paragraphs [0004], [0011], [0053] and states that when combined with Messerges, these passages show parts of limitations (h) and (i) ("disable request causes the license corresponding to the locked content data to be disabled" and "said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network.").

The relevant passages of Chase and Yaacovi are recited here:

> [Chase 0020] In the present invention, content revocation is achieved by disabling all licenses issued to a user's computing device for corresponding content. Since the DRM system on the computing device acts based on received licenses, a content revocation is delivered within such a license. Upon storage of a license containing a content revocation on the computing device, the DRM system recognizes the content revocation within the license, validates the content revocation, and stores same in the secure state store under the public key of the content server (PU-CS). Importantly, each license has a (PU-CS) therein, and each evaluation of a license considers each content revocation stored in the state store and having the same (PU-CS), and determines based on the content revocation whether such license is to be disabled or otherwise affected. A content revocation is one form of a license modification that may be delivered within a license.
>
> [Chase 0279] In accordance with the DRM architecture as set forth above, content revocation is achieved by disabling all licenses 16 issued to a user's computing device 14 for the content 12. Since the DRM system 32 on the computing device 14 acts based on received licenses 16, the content revocation is delivered within such a license 16. Upon storage of a license 16 containing a content revocation on the computing device 14, the DRM system 32 recognizes the content revocation within the license 16, validates the content revocation, and stores same in the secure state store 40 under the public key of the content server 22 (PU-CS).

Importantly, each future evaluation of a license 16 considers all content revocations stored in the state store and determines whether such license 16 is bound to content 12 that has been disabled according to a particular content revocation. If so, the license 16 refuses to allow rendering of the content 12.

[Chase 0283] In one embodiment of the present invention, and referring now to FIGS. 13 and 14, the content owner effectuates such a revocation by first generating a revocation string 60 containing revocation information (step 1301), and delivers the revocation string 60 to a license server 24 (step 1303). Note that the license server 24 that receives the revocation string need not necessarily be the license server 24 that issued the corresponding licenses 16 to be revoked. Accordingly, the revocation string 60 may be delivered to multiple license servers 24.

[Yaacovi 0004] The problem of copying digital content is exacerbated by the fact that digital content cannot easily be "re-sold." In the physical world, a book, analog videocassette, audio vinyl disk recording, etc., can be sold from its original owner to a secondhand purchaser. This may be an advantageous transaction for both parties: the secondhand purchaser acquires a used copy of a book, record, videocassette, etc. at a reduced price as compared with the cost of a new copy, and the seller may be able to get some money for an item that he or she no longer needs or wants. This situation has no analogue in the digital world. A first user of digital content generally transfers that content to a second user by making a copy of the content (e.g., by copying it to a floppy disk, or transmitting a copy over the Internet). Once the copy is made, the first user has no incentive to destroy the old copy, since both copies are equally good and equally usable. In other words, in contrast with the physical world, transfer of content in the digital world does not normally deprive the original owner of the content. Thus, a person who wants to acquire a copy of digital content must purchase it new or make an (often illegal) copy. In theory, the legal terms of a copyright license for the content may require payment to the owner of the content at the time the copy is made, but compliance with such terms is rare at best.

[Yaacovi 0011] Relicensing terms other than the one

described above may also be used. For example, a relicensing term could permit resale of the content and require revocation of the original license as a condition to the sale. This term could be enforced by requiring that, at the time of relicensing, the licensing authority instruct the first user's computer to void the original license. It should further be appreciated that the above-described technique can be adapted for use with all types of content--e.g., text, audio, video, multimedia, software, etc.

[Yaacovi 0053] Once download server 180a has the relevant information, it proceeds to enforce the terms of the relicensure. For example, download server 180a may verify in its records that content package 204 has not been previously sold by the owner identified in term 302, since exemplary relicensing term 308 only permits one resale of content package 204. Assuming that relicensure of the content is permitted, download server 180a may engage in a credit card transaction with computing device 110b in order to collect the specified "resale" payment (eight dollars, in this example). After payment is collected, download server 180a may contact computing device 110a in order to provide the two dollar payment to which the original content owner is entitled under the terms of licensing term 308 (or may arrange for this payment to be deposited in some other place.) Other actions may also be taken depending on the conditions of relicensure specified in the relicensing term(s). For example, as noted above, a true "used book sale" scenario may be created whereby the original licensee's license is revoked upon resale; in this case, the download server may contact computing device 110a to instruct computing device 110a to revoke the original owner's license. (This revocation may be performed by rendering application 145a, which may be configured to rewrite license 206 in response to such an instruction.) When download server 180a has fulfilled the conditions upon which content package 204 is to be relicensed, it relicenses content package 204 for use on computing device 110b. The act of relicensing may occur in various ways. The following is a non-exhaustive list of ways that content package 204 can be relicensed for use on computing device 110b:

Appellants respectfully disagree with the Examiner's characterization of the combination of Messerges, Chase, and Yaacovi. The above quoted passages of Chase and Yaacovi merely state that content revocation is achieved by disabling all licenses and that license revocation is required for the resale of the content. The combination of these two references with Messerges neither teaches nor suggests that the locked content data is changed to a discrete instance when the locked content data is to be moved to another server device bound to another hub network, that the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and that the disable request causes the license corresponding to the locked content data to be disabled as claimed in limitations (h) and (i) of claim 1.

Further, it should be noted that the combination of Messerges, Chase, and Yaacovi as explained by the Examiner still fails to cover the limitation that when the server sends a disable request it is a request to change the bound instance of the locked content data to the discrete instance. These two types of instances are useful in hub networks. For example, according to page 7, line 26 to page 8, line 19 of Appellants' specification as filed, "Compliant media operates according to the processes defined for content that can be ingested into (made bound) and freed from (made discrete) a hub network." Also, according to page 28, line 10 to page 29, line 22 of Appellants' specification as filed: "A discrete instance of content is not bound to any hub network and can be moved from one device to another, in or out of the hub network, using compliant media." None of the references mention the changing of the instances.

The Examiner states in the Advisory Action dated December 22, 2010 that the "characterization of the art entails that a content license is revoked on a client device via a server, as per Chase JR et al. (0279, 0280, 0288). The characterization of the prior art illustrates an example of when content can be revoked, such as selling the content to another user. When this occurs, a license for the original content is revoked such that a user in one domain no longer may use the content. In effect, the request to disable a license is predicated on a request to sell content within the domain. As modified, the

server receives the request to disable a license based on information indicating content is to be sold from its domain. As a result of revoking the license for the content in the first domain, the content is rendered discrete or independent of the first domain, because the domain no longer has rights to the content. The prior art of record also illustrates that client devices may act as a server/client. A user of another domain, upon purchasing the content from the first domain, is able render such content upon receiving a license from its server." The Examiner further states in the Advisory Action that with "regard to the limitation to changing a bound instance to a discrete instance, this occurs upon disabling a license for the content that is to be sold from the first domain to another user. It is the license revocation that results in the bound content, i.e., licensed content to a first domain, to be changed to a discrete instance, i.e., not licensed for use in he first domain and therefore independent." Appellants respectfully disagree with this characterization in that Chase fails to teach or suggest changing the locked content data from a bound instance to a discrete instance as a result of revoking the license of the locked content data. Chase does not provide any suggestion that somehow the state of the locked content data will be changed from bound to discrete by revoking the license.

Regarding claim 2, it recites that "said locked content data and said license corresponding to said locked content data are stored on the server device." This limitation is disclosed on page 5, line 20 to page 6, line 6 of the application as follows: "The bound instance is one logical instance represented by locked content data and corresponding licenses stored on the server of the hub network and on zero or more of the clients of the hub network." The Office Action indicates that the limitations of claim 2 are taught by paragraphs [0042]-[0049] of Messerges and paragraph [0080] of Foster. The Office Action further states "requested content is provided from a content provider. The requested content, as part of the content package, further includes an electronic rights table, a rights document, encrypted content....The objects of the content package may optionally be provided by two files - a license file, encoded rights table, and an encrypted content, etc. As modified by Foster, such locked content would be stored on a participating device that functions as both a server and authorizer, supra Foster [COL [0080]]." However, the combination of passages of Messerges and Foster fails to teach or suggest that the locked content data

and the license corresponding to the locked content data are stored on the server device.

Regarding claim 5, a further limitation is added to claim 1 to check that the license includes sending a confirmation license request to the server from the client. The Office Action indicates that the limitations of claim 5 are taught by paragraphs [0060]-[0061] of Messerges. The Office Action further states "a content package is opened via verifying the package's rights document, hash, and encoded rights table....As applied to Foster, a server authorizer device includes the aforementioned function of checking a license prior to distributing content to the participating device." However, these passages of Messerges fail to teach or suggest that the license includes sending a confirmation license request to the server from the client.

Regarding claim 7, a further limitation is added to claim 5 to check a revocation list to determine whether the client is included in the revocation list, wherein the revocation list (stored on the server) indicates devices for which the license has been revoked. This limitation is disclosed on page 20, lines 8-12 of the application as follows:

> [Page 20, lines 8-12] In one implementation, the server also confirms that the client device is not on the server's revocation list before authorizing the client device. As described below, the revocation list indicates devices for which authorization has been revoked. In one implementation, the server adds the authorized client device to a list of authorized devices.

The Office Action indicates that claim 7 is disclosed in paragraphs [0073], [0029], and [0063]-[0064] of Messerges. However, these paragraphs of Messerges fails to teach or suggest checking a revocation list to determine whether the client is included in the revocation list, wherein the revocation list (stored on the server) indicates devices for which the license has been revoked.

Based on the foregoing discussion, claims 1, 2, 5, and 7 should be allowable over the combination of Messerges, Foster, Chase, and Yaacovi. Further, since independent claim 14 recites similar limitations as recited in claim 1, claim 14 should also be allowable over

the combination of Messerges, Foster, Chase, and Yaacovi. Since claims 3, 6, 8-13, and 15-18 depend from one of claims 1 and 14, claims 3, 6, 8-13, and 15-18 should also be allowable over the combination of Messerges, Foster, Chase, and Yaacovi.

Accordingly, the Board should reject these improper assertions as explained above.

B. Claims 19-28 are not unpatentable over Messerges in view over Russell, in view over Foster, in view over Chase, and in further view over Yaacovi under 35 U.S.C. §103(a)

In the Office Action, claims 19-28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Messerges in view over Russell, in view over Foster, in view over Chase, and in further view over Yaacovi. As explained in the Manual of Patent Examination Procedure §706.02, entitled Rejection on Prior Art, for obviousness under 35 U.S.C. §103, "to support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." As set forth in detail below, the outstanding rejections are improper because the cited references do not suggest the claimed invention either explicitly or impliedly, or the examiner did not present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the cited references.

Based on the foregoing discussion regarding claim 1, and since independent claims 19 and 26 recite similar limitations as recited in claim 1, claims 19 and 26 should also be allowable over the combination of Messerges, Foster, Chase, and Yaacovi. Further, Russell is merely cited for allegedly teaching "a main server containing copy of each content item". Thus, claims 19 and 26 should be allowable over the combination of Messerges, Russell, Foster, Chase, and Yaacovi. Further, since claims 20-25 and 27-28 depend from claims 19 and 26, respectively, claims 20-25 and 27-28 should also be allowable over the combination of Messerges, Russell, Foster, Chase, and Yaacovi.

Accordingly, the Board should reject these improper assertions as explained above.

C. **Claims 29-39 are not unpatentable over Messerges in view over Foster, and in further view over Russell, in view over Chase, in view over Yaacovi and in further view over Peinado under 35 U.S.C. §103(a)**

In the Office Action, claims 29-39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Messerges in view over Foster, and in further view over Russell, in view over Chase, in view over Yaacovi and in further view over Peinado. As explained in the Manual of Patent Examination Procedure §706.02, entitled Rejection on Prior Art, for obviousness under 35 U.S.C. §103, "to support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." As set forth in detail below, the outstanding rejections are improper because the cited references do not suggest the claimed invention either explicitly or impliedly, or the examiner did not present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the cited references.

Based on the foregoing discussion regarding claim 19 and 26, and since independent claim 37 recites similar limitations as recited in claims 19 and 26, claim 37 should also be allowable over the combination of Messerges, Russell, Foster, Chase, and Yaacovi. Further, Peinado is merely cited for allegedly teaching that "a license store may be embodied in any other form so long as the license store performs the function of storing license in a location convenient for the DRM". Thus, claims 26 and 37 should be allowable over the combination of Messerges, Russell, Foster, Chase, Yaacovi, and Peinado. Further, since claims 29-36 and 38-39 depend from claims 26 and 37, respectively, claims 29-36 and 38-39 should also be allowable over the combination of Messerges, Russell, Foster, Chase, Yaacovi, and Peinado.

Accordingly, the Board should reject these improper assertions as explained above.

CONCLUSION

In view of the foregoing, Appellants respectfully submit that the claimed invention is patentable over the references of record. The Examiner has failed to identify or provide teachings in the references for each of the claim limitations. Appellants respectfully request reversal of the Examiner's rejections.

Respectfully submitted,

Dated: 2-7-11

By: 
Samuel S. Lee
Reg. No. 42,791

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101-4469
(619) 525-3821
Customer No. **27189**

(viii) Claims Appendix

1. A method of presenting content data, comprising:

receiving at a server device a present request indicating locked content data from a client connected to a hub network,

wherein the server device is configured to set up the hub network including adding the client and the server device to the hub network,

wherein the server device is configured to function as a client in the hub network, and

wherein said locked content data is stored on the server device connected to the hub network;

checking a license corresponding to said locked content data to determine if said license permits said client to present said locked content data,

wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said client connected to the hub network,

wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and

wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server device bound to another hub network, the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled; and

presenting said locked content data through a presentation component connected to said client when said locked content data is a bound instance.

2. The method of claim 1, wherein:

said locked content data and said license corresponding to said locked content data are stored on the server device.

3. The method of claim 2, wherein:

presenting said locked content data includes decrypting said locked content data to produce output content data and sending said output content data to said presentation component.

4. (Canceled)

5. The method of claim 1, wherein:

checking said license includes sending a confirm license request to the server device from said client.

6. The method of claim 5, wherein:

presenting said locked content data includes receiving output content data streamed from said server device to said client.

7. The method of claim 5, further comprising:

checking a revocation list to determine whether said client is included in said revocation list;

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said server device.

8. The method of claim 1, further comprising:

checking a revocation list to determine whether said client is included in said revocation list;

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said client.

9. The method of claim 1, wherein: said locked content data is media data.

10. The method of claim 1, wherein: said presentation component is integral to said client.

11. The method of claim 1, wherein: said presentation component is external to said client.

12. The method of claim 1, wherein: said presentation component includes a television.

13. The method of claim 1, wherein: said presentation component includes an audio speaker system.

14. A method of presenting content data, comprising:

receiving at a server connected to a hub network a present request indicating locked content data and indicating to a client connected to said hub network to present the content data,

wherein the server is configured to set up the hub network including adding the client and the server to the hub network,

wherein the server is configured to function as a client in the hub network, and

wherein said locked content data is stored on the server connected to the hub network;

checking a license corresponding to said locked content data to determine if said license permits said server to present said locked content data through said client,

wherein said locked content data is a bound instance if said license permits presentation of said locked content data by said server through said client connected to the hub network,

wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and

wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network, the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled; and

presenting said locked content data by streaming data to said client when said locked content data is a bound instance.

15. The method of claim 14, wherein: streaming data to said client includes streaming locked content data to said client.

16. The method of claim 14, further comprising:

decrypting said locked content data.

17. The method of claim 14, wherein: said present request is received from said client.

18. The method of claim 14, further comprising:

checking a revocation list to determine whether said client is included in said revocation list;

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said server.

19. A method of copying content data, comprising:

receiving in a hub network a copy request indicating locked content data,

wherein the hub network includes a server configured to set up the hub network including adding the client and the server to the hub network, and

wherein the server is configured to function as a client in the hub network and wherein said locked content data is stored on the server; and

copying said locked content data to produce a copy of said locked content data when said locked content data is a bound instance with a corresponding license that is bound to said hub network;

wherein the bound instance of said locked content data and the license corresponding to said locked content data are bound to the hub network, and

wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network,the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled.

20. The method of claim 19, further comprising:

checking said license to determine if said license permits said locked content data to be copied.

21. The method of claim 19, further comprising:

requesting a new license from the server for said copy of said locked content data;

wherein said server is in said hub network and connected to said client.

22. The method of claim 19, further comprising:

sending said copy of said locked content data to a device that is not a member of said hub network.

23. The method of claim 19, further comprising:

sending said copy of said locked content data to a client that is a member of said hub network but is not connected to said hub network.

24. The method of claim 19, further comprising:

sending a new license to a client that is a member of said hub network but is not connected to said hub network.

25. The method of claim 19, further comprising:

checking a revocation list to determine whether said client is included in said revocation list;

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said client.

26. A method of distributing content data, comprising:

receiving from a providing device connected to a hub network, and at a receiving device a copy of locked content data that is a bound instance bound to said hub network,

wherein the providing device is configured to set up the hub network including adding the receiving device and the providing device to the hub network,

wherein the providing device is configured to function as a receiving device in the hub network, and

wherein said locked content data is stored on the providing device connected to the hub network;

requesting a new license for said copy of locked content data; and

receiving said new license for said copy of locked content data of the bound instance bound to said hub network,

wherein the bound instance of said copy of locked content data and the new license corresponding to said copy of locked content data are bound to the hub network, and

wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network, the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the

discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled.

27. The method of claim 26, wherein: said providing device is a client in said hub network.

28. The method of claim 26, wherein: said providing device is a server in said hub network.

29. The method of claim 26, wherein: said new license is received from said client.

30. The method of claim 26, wherein: said new license is received from a server in said hub network.

31. The method of claim 26, wherein: said new license is received from an external server that is not in said hub network.

32. The method of claim 26, wherein:

said copy of locked content data has corresponding licensing authority information stored on said providing device, and

said new license is received from a licensing authority indicated by said licensing authority information.

33. The method of claim 26, wherein: said receiving device is not a member of said hub network.

34. The method of claim 26, wherein: said receiving device is a member of a second hub network, and said new license of said copy of locked content data is bound to said second hub network but not to said hub network.

35. The method of claim 26, wherein: said receiving device is not connected to said hub network.

36. The method of claim 26, further comprising:

checking a revocation list to determine whether said receiving device is included in said revocation list;

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said receiving device.

37. A method of distributing content data, comprising:

receiving at a server connected to a hub network, and from a device a request for a new license for a copy of locked content data that is a bound instance bound to said hub network,

wherein the server is configured to set up the hub network including adding the client and the server to the hub network,

wherein the server is configured to function as a client in the hub network, and

wherein said locked content data is stored on the server connected to the hub network;

checking a root license stored on said server to determine if said root license permits said server to provide a new license for said copy of locked content data of the bound instance; and

creating said new license according to said root license;

sending said new license to said device,

wherein said new license for said copy of locked content data of the bound instance is bound to said hub network,

wherein the bound instance of said copy of locked content data and the new license are bound to the hub network, and

wherein said locked content data is changed to a discrete instance when said locked content data is to be moved to another server bound to another hub network, the server device sends a disable request for the locked content data to clients of the hub network to indicate that the bound instance of the locked content data is changed to the discrete instance, and wherein the disable request causes the license corresponding to the locked content data to be disabled.

38. The method of claim 37, wherein: said device is not connected to said hub network.

39. The method of claim 37, further comprising:

checking a revocation list to determine whether said device is included in said revocation list;

wherein said revocation list indicates devices for which the license has been revoked, and

wherein said revocation list is stored on said server.

40. (Canceled)

(ix) Evidence Appendix

None.

(x) Related Proceedings Appendix

None.